REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Amendments to Claim 1

The amendments to claim 1 are for the purpose of more positively reciting the processing station, card, and card "initialization," by moving the recitations of the processing station, card, and card "initialization" from the preamble of the claim to the body of the claim, and also to clarify that it is not the "initial secret value" that is exchanged, but rather the values used to determine the "initial secret value."

The amendments are in response to the Examiner's comments in item 8 on page 6 of the Official Action that the Examiner did not give "patentable weight" to the recitation of card initialization because the recitation of card initialization was previously included only in the preamble of claim 1, and also in response to comments by the Examiner concerning the exchange of secret values (as opposed to the respective "determination" of secret values by the processor and card).

It is respectfully submitted, since the issues of card initialization and exchange of secret values were either raised by the Examiner or previously considered, and since the amendment is limited to this particular issue, that the amendment to claim 1 does not raise any **new issues**, and further that the amendment should be entered since it places the application in better condition for appeal. The amendment clearly does not involve new matter since the changes are essentially formal in nature.

2. Rejection of Claims 1 and 3-8 Under 35 USC §103(a) in view of U.S. Patent Nos. 4,200,770 (Hellman) and 6,038,551 (Barlow)

This rejection is again respectfully traversed on the grounds that neither the Hellman patent nor the Barlow patent, whether considered individually or in any reasonable combination, discloses or suggests a chipcard initialization step in which:

- parts of respective first and second "values" are respectively generated by the card *and* processing station;
- the processing station determines a secret initial value from at least part of the first value and the transmitted part of the second value; and
- the chip card determines the same secret initial value from at least part of the second value and the transmitted part of the first value, *without the need to actually exchange any part of the secret "initial" value used to initialize the card.*

The point of the present invention is that no part of the secret initial value is exchanged during initialization. Instead, the processing station determines the secret value and the chip card also determines the secret value without ever exchanging any part of the secret value. All calculations that result in determination of the secret initial value are performed in parallel by processor and the chip card. All that are transmitted are parts of values used in the generation of the secret initial value. If an eavesdropper does not know the calculations used to generate the initial secret value from the transmitted values, then the eavesdropper cannot possibly generate the initial secret value from the exchanged values.

In the "Response to Arguments" section of the Official Action, the Examiner refers to "applicant's suggestion that the cited references fail to disclose transferring 'parts' of secret initial value (pages 6-8 of applicant's response) [*sic.*]." This paraphrase of the arguments made in the last response is exactly **contrary** to the actual arguments made by applicant. **The applicant has never suggested that the cited references fail to disclose transferring 'parts' of a secret initial value, as alleged in item 9 on pages 6-7 of the Official Action.** To the contrary, the difference between the claimed invention and the prior art is that the prior art,

including the Diffie-Hellman algorithm, is required to exchange at least parts of secret values, whereas the claimed invention seeks to generate the secret value in the first place, and does not require any transmission of a part of the secret value.

It is true that use of the term "exchange" in describing the determination of secret values was somewhat confusing. The purpose of the claimed invention is to replace the usual "exchange" with parallel determination of the initial secret value, the result being the same as an exchange (initial secret values shared by the card and processor), without the actual transfer (whether or not encrypted) of parts of the secret value.

The purpose of a Diffie-Hellman key exchange, on the other hand, is to enable both parties to use pre-stored secret keys. Unlike a Diffie-Hellman "exchange," the present invention is concerned the problem of how to store the secret keys in the first place. The method of the invention does not exchange parts of secret keys, but rather has a chip card generate its own key based on generated value, which does not need to be secret since the part of the generated value used calculate the secret key is not transmitted, and a transmitted part of a value generated by the processing station, which also does not need to be secret because the part of the value generated by the processing station that is used to re-create the key on the processing station side is also not transmitted.

In the system of Hellman (cited by the Examiner as teaching the claimed generation of secret initial values from a part of a transmitted value and part of a received value), the secret signal is already possessed by each party to the transaction, and therefore when the parts of the secret signal are exchanged for verification, they must be encrypted or "transformed" so that an eavesdropper cannot reconstruct the secret signal from the transmitted parts. This has an entirely different effect than the exchange of the present invention.

Contrary to the allegation in item 7 on pages 5-6 of the Official Action, the Hellman patent does not teach, in col. 4, lines 53-67, the generation of parts of respective first and second

values by the card and processing stations and, in col. 4, lines 44-67, the determination of a secret initial value, ***by both the processing station and the card***, from at least part of a first/second value and the transmitted part of the second/first value. Instead of generating a **secret initial value**, the method of Hellman actually requires a secret initial value to **already be present** on the card, so that the transformed values used to generate a session key can be safely exchanged. The method of Hellman therefore cannot be used for initialization.

As explained in the previous response, in the system of Hellman, the "conversers" already "***each*** *possess a secret signal and exchange an initial transformation of the secret signal with the other converser*" (see, *e.g.*, the abstract of Hellman). While the secret signals of Hellman correspond to the secret values of the claimed invention in the sense that they can be used to facilitate further encrypted communications, and in particular the generation of shared secret keys, these secret signals must themselves actually be exchanged in order to enable subsequent key exchanges. **Unlike the claimed invention, which only transmits parts of respective first and second values used in the determination of the secret initial value, Hellman takes the approach of protecting the "secret signals" by "transforming" the secret signals before their exchange.** While such exchanges can be made relatively secure through the use of one-way function transformations, the protection is not perfect. In contrast, the claimed invention does **not** require any exchange of the secret values, whether ***transformed*** or not. Instead, only parts of the values are exchanged.

These deficiencies of the Hellman patent are not remedied by the Barlow patent, which teaches a system that not only exchanges secret keys, but does so by means of public key encryption of the exchanged secret keys. Barlow makes no attempt to only exchange parts of secret values, but rather simply encrypts all of the values before exchange (col. 3, lines 1-13). This public key method of Barlow is not suitable for chipcard initialization of the type claimed, and Barlow does not even remotely suggest a method of generating an initialization value without exchanging the values.

In the claimed invention, initial values can be generated for each chipcard manufactured in a relatively simple and yet secure manner. Barlow, on the other hand, points out the difficulty of providing millions of different devices with individual keys. This is hardly suggestive of a method that might be applied to chipcard initialization, or of a method that could be combined with the secret value generation and exchange of Hellman to obtain the claimed invention.

Because neither the Hellman patent nor the Barlow patent discloses or suggests ***generation of*** *secret values by both a processing station and a chip card based on partial exchange of non-secret values prior to initialization,* it is respectfully submitted that no combination of the Hellman and Barlow patents could possibly have suggested the claimed invention to the ordinary artisan, and withdrawal of the rejection of claims 1 and 3-8 under 35 USC §103(a) is respectfully requested.

4. Rejection of Claim 2 Under 35 USC §103(a) in view of U.S. Patent Nos. 4,200,770 (Hellman) and 6,038,551 (Barlow), "*Cryptographic Identification Methods For Smart Cards In the Process of Standardization*" (Konigs), and *Handbook of Applied Cryptography* (Menezes)

This rejection is respectfully traversed on the grounds that the Menezes and Konigs articles, like the Hellman and Barlow patents, fail to disclose or suggest a chipcard initialization method in which secret values are established for the chipcard and processor to use in subsequent communications, such as for use in transferring a secret key to the card, *without an exchange of the "secret values,"* by exchanging only parts of values generated by the chipcard and processor.

Instead, the Konigs article, again like the Hellman and Barlow patents, discloses a method of establishing cryptographic data connections using chipcards without containing any suggestion as to how the chipcards used for the cryptographic data connections are initialized for use in the cryptographic connections, while the Menezes publication merely teaches the use of sequence numbers to identify entities in key establishment protocols, and does not teach any specific initialization method of the type claimed. As a result, withdrawal of the rejection of claim 2 under 35 USC §103(a) is respectfully requested.

5. Rejection of Claim 9 Under 35 USC §103(a) in view of U.S. Patent Nos. 4,200,770 (Hellman), 6,038,551 (Barlow), and 5,224,163 (Gasser)

This rejection is again respectfully traversed on the grounds that the Gasser patent, like the Hellman patent and the Barlow patent, fails to disclose a card initialization step in which transfer of data to the card is facilitated by a "secret value" exchange that only involves transfer of "parts" of the respective secret values, and that does not require transformation of the secret values. Instead, the Gasser patent disclose generation of "session public/private encryption key pairs." The session public/private key pairs are generated, as is common in such session key generating schemes, by mutual exchange and processing of secret values, but there is no disclosure in the Gasser patent that the secret values used in the public/private session key generating process may be transferred to the chipcard by a secret value generated in the manner claimed, using parts of two picnics in the manner claimed. Accordingly, withdrawal of the rejection of claim 9 under 35 USC §103(a) is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,
BACON & THOMAS, PLLC

Date: May 4, 2004

By: BENJAMIN E. URCIA
Registration No. 33,805

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500